

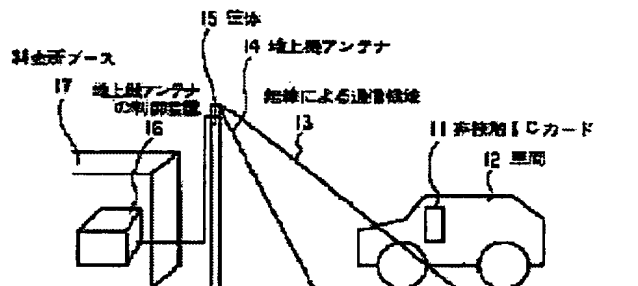
## NONCONTACT IC CARD SYSTEM

**Patent number:** JP8221624  
**Publication date:** 1996-08-30  
**Inventor:** KATO MASAKI; FUJITA ICHIRO; YAMAMOTO KIMIYUKI  
**Applicant:** MITSUBISHI HEAVY IND LTD  
**Classification:**  
- **international:** G07B15/00; G07B15/00; G06K17/00; G07F7/08; G08G1/017  
- **european:**  
**Application number:** JP19950028134 19950216  
**Priority number(s):**

### Abstract of JP8221624

**PURPOSE:** To provide a noncontact IC card which can maintains the security on a radio line with a ground equipment antenna.

**CONSTITUTION:** As for the noncontact IC card system of toll reception system which allows vehicles to travel on a toll highway on a non-stop and cashless basis, a noncontact IC card 11 consists a ciphering algorithm execution unit for message ciphering and a secret key storage memory for ciphering, and the ground equipment antenna 14 also consists of a ciphering algorithm execution unit and a secret key storage memory for ciphering, and messages sent from both the noncontact IC card 11 and ground equipment antenna 14 are ciphered, key numbers are also sent as the contents of the messages at the same time, and keys for ciphering are updated, message by message, to improve the secrecy of exchanged messages.



Data supplied from the *esp@cenet* database - Worldwide

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-221624

(43) 公開日 平成8年(1996)8月30日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 7 B 15/00	5 1 0		G 0 7 B 15/00	5 1 0
				G
				J
G 0 6 K 17/00			G 0 6 K 17/00	L
				F

審査請求 未請求 請求項の数2 O L (全 7 頁) 最終頁に続く

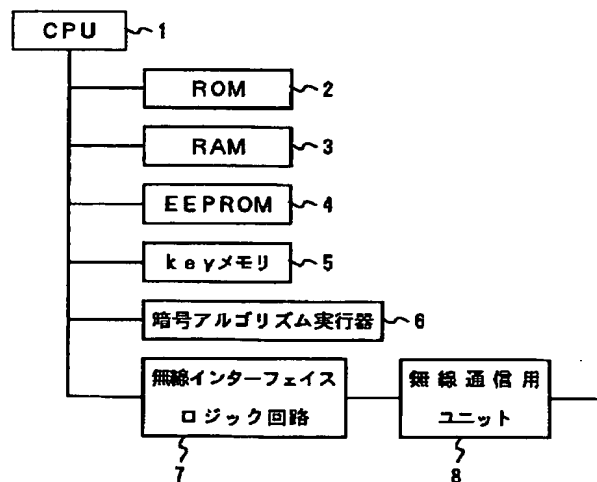
(21) 出願番号	特願平7-28134	(71) 出願人	000006208 三菱重工業株式会社 東京都千代田区丸の内二丁目5番1号
(22) 出願日	平成7年(1995)2月16日	(72) 発明者	加藤 聖樹 兵庫県高砂市荒井町新浜二丁目1番1号 三菱重工業株式会社高砂研究所内
		(72) 発明者	藤田 一郎 兵庫県神戸市兵庫区和田崎町一丁目1番1号 三菱重工業株式会社神戸造船所内
		(72) 発明者	山本 公之 兵庫県神戸市兵庫区和田崎町一丁目1番1号 三菱重工業株式会社神戸造船所内
		(74) 代理人	弁理士 鈴江 武彦

(54) 【発明の名称】 非接触 I C カードシステム

## (57) 【要約】

【目的】本発明は、地上機アンテナとの無線回線上のセキュリティを守ることができる非接触 I C カードシステムを提供することを目的とする。

【構成】本発明に係る非接触 I C カードシステムは、有料自動車道路をノンストップかつキャッシュレスで通行できる料金収受システムの非接触 I C カードシステムにおいて、非接触 I C カード 1 1 は、メッセージ暗号化のための暗号アルゴリズム実行器 6 と、暗号化のための機密キー格納メモリ 5 により構成され、地上機アンテナ 1 4 も、暗号アルゴリズム実行器 6 と、暗号化のための機密キー格納メモリ 5 により構成されることにより、非接触 I C カード 1 1 と地上機アンテナ 1 4 の双方から発信されるメッセージを暗号化し、キー番号 9 も同時にメッセージの内容として発信し、メッセージごとに暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。



## 【特許請求の範囲】

【請求項1】 有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ICカードシステムにおいて、(A)非接触ICカード(11)は、メッセージ暗号化のための暗号アルゴリズム実行器(6)と、暗号化のための機密キー格納メモリ(5)により構成され、(B)地上機アンテナ(14)も、暗号アルゴリズム実行器(6)と、暗号化のための機密キー格納メモリ(5)により構成されることにより、(C)非接触ICカード(11)と地上機アンテナ(14)の双方から発信されるメッセージを暗号化し、(D)キー番号(9)も同時にメッセージの内容として発信し、(E)メッセージごとに、暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする非接触ICカードシステム。

【請求項2】 有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ICカードシステムにおいて、(A)非接触ICカード(11)は、メッセージ暗号化のための暗号アルゴリズム実行器(106)と、暗号化のための機密キー格納メモリ(105)と、ランダムナンバー発生器(107)により構成され、(B)地上機アンテナ(14)も、暗号アルゴリズム実行器(106)と、暗号化のための機密キー格納メモリ(105)と、ランダムナンバー発生器(107)により構成されることにより、(C)ランダムナンバー発生器(107)で乱数を発生させ、(D)前記ランダムナンバーと任意に選択したマスターキー(113)により、暗号化関数を実行して、一時キーを作成し、(E)前記一時キーと、非接触ICカード(11)と地上機アンテナ(14)の双方から発信させるメッセージを暗号化し、(F)さらに選択したキー番号と乱数も同時にメッセージの内容として発信し、(G)メッセージごとに、暗号化のためのキーと乱数を更新することにより、交換されるメッセージの機密性を向上させることを特徴とする非接触ICカードシステム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、有料道路の料金収受に利用される非接触ICカードシステムに関する。本発明は、上記以外にも物流・入退出管理システムなど、特にセキュリティが要求される分野にも利用することができ

## 【0002】

【従来の技術】近年、有料道路での交通渋滞緩和・料金収受業務の省力化の一案として非接触ICカードシステムの実用化研究が盛んに実施されている。図6は、近年の非接触ICカードシステムの運用メッセージを示したものである。図6において、11は非接触ICカードを

示したものであり、車両12に搭載されて、非接触ICカードシステム使用可能な料金所ゲートに進入する事になる。

【0003】14は地上機アンテナであり、筐体15に支持されている。13は地上機アンテナが作り出す非接触ICカードとの無線による通信領域である。

【0004】16は地上機アンテナを制御する、アンテナ制御装置である。17は料金所ブースである。このような、非接触ICカード使用可能な料金所ゲートに車両12が進入した場合、非接触ICカードは、地上機アンテナが出力する問合せメッセージに応答して、固有情報を地上機アンテナに返信することになる。

【0005】この固有情報の中には、非接触ICカードのIC番号や、車種区分、入口料金所の情報などの重要なデータを含んでいる。地上機アンテナおよびアンテナ制御装置では、その情報を受信し、課金値(通行料金)を計算し、非接触ICカードに返送することになる。

【0006】非接触ICカードでは、その課金値を受信し、内部の記録媒体から課金値を減算し、新残額に更新することになる。図7は、従来の非接触ICカードの内部ブロック図を示したものである。図7において、220は非接触ICカードのCPUである。

【0007】221はプログラム用のROM、222は作業用もしくは、データー時記憶用のRAMである。223は、金額を電氣的に記憶するEEPROMである。

【0008】224は、無線通信用で受信したシリアルデータをパラレルデータに変換したり、CPUのデータを無線通信用に加工したりする無線通信用ロジックである。225は、無線通信のためのアナログユニットであり、データ復調回路、データ変調回路などより構成されている。

## 【0009】

【発明が解決しようとする課題】ところが上記、従来の非接触ICカードでは、非接触ICカードと地上機アンテナとの無線回線上のセキュリティは、何ら考慮されていなかった。つまり、地上機から送信される問合せメッセージも、課金処理メッセージも、非接触ICカードから返送されるIDメッセージもすべて、一般的に知識のある人が認識可能なメッセージ(平文)でやりとりされていた。

【0010】このような事態は、金額情報を扱う料金所システムにおいては、懸念されるべきである。なぜならば、このメッセージの盗聴者は、容易にこのメッセージを理解でき、もし意図すれば、メッセージの一部を、有利なメッセージに交換したりして、正常の課金値よりも格安でもしくは、無料で料金所ゲートを通することも可能である。本発明は、これらの問題を解決することができ非接触ICカードシステムを提供することを目的とする。

## 【0011】

## 【課題を解決するための手段】

(第1の手段) 本発明に係る非接触 IC カードシステムは、有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触 IC カードシステムにおいて、(A) 非接触 IC カードは、メッセージ暗号化のための暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリにより構成され、(B) 地上機アンテナも、暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリにより構成されることにより、

(C) 非接触 IC カードと地上機アンテナの双方から発信されるメッセージを暗号化し、(D) キー番号も同時にメッセージの内容として発信し、(E) メッセージごとに、暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。

(第2の手段) 本発明に係る非接触 IC カードシステムは、有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触 IC カードシステムにおいて、(A) 非接触 IC カードは、メッセージ暗号化のための暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリと、ランダムナンバー発生器により構成され、(B) 地上機アンテナも、暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリと、ランダムナンバー発生器により構成されることにより、(C) ランダムナンバー発生器で乱数を発生させ、

(D) 前記ランダムナンバーと、任意に選択したマスターキーにより、暗号化関数を実行して、一時キーを作成し、(E) 前記一時キーと、非接触 IC カードと地上機アンテナの双方から発信させるメッセージを暗号化し、

(F) さらに、選択したキー番号と乱数も同時にメッセージの内容として発信し、(G) メッセージごとに、暗号化のためのキーと乱数を更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。

## 【0012】

## 【作用】

(請求項1に係る発明の作用) 本発明の非接触 IC カードシステムによれば、地上機アンテナからのメッセージには先頭にキー（以下 Key という）番号が付加されている。

【0013】その後続くデータは、この Key 番号で指定された機密 Key で暗号化されている。非接触 IC カードでは、この機密メッセージを受信すると、最初に Key 番号を認識し、この Key 番号で指定された機密 Key を Key メモリの中から検索し、暗号アルゴリズム実行器に入力する。

【0014】この暗号アルゴリズム実行器に、同時に受信した機密データを入力することにより出力として、平文の認識可能なメッセージを得ることができる。非接触 IC カードが地上機アンテナに返信する際も同様であ

る。

【0015】非接触 IC カードは、任意に Key メモリの中から機密 Key を選択し、その Key でデータを暗号化して、その Key のインデックスである Key 番号とともに地上機に返信する。

(請求項2に係る発明の作用) 本発明の非接触 IC カードシステムによれば、地上機アンテナからのメッセージには先頭に Key 番号が付加されている。

【0016】その後、数バイトは乱数が発信される。更にその後続くデータは、この Key 番号で指定された機密 Key と乱数を暗号化関数で実行した一時 Key で暗号化されている。

【0017】非接触 IC カードでは、この機密メッセージを受信すると、最初に Key 番号を認識し、この Key 番号で指定された機密 Key を Key メモリの中から検索し、暗号アルゴリズム実行器に入力する。

【0018】次に、受信された乱数を同時に暗号アルゴリズム実行器に入力し、出力として一時 Key を得ることができる。その後、この一時 Key と、同時に受信した機密データを、再び暗号化アルゴリズム実行器に入力することにより、出力として、平文の認識可能なメッセージを得ることができる。

【0019】非接触 IC カードが地上機アンテナに返信する際も同様である。非接触 IC カードは、任意に Key メモリの中から機密 Key を選択し、更に乱数を発生させ、暗号化アルゴリズム発生器に入力し、一時 Key を作成する。その Key でデータを暗号化して、もとの機密 Key の Key 番号と、数バイトの乱数とともに地上機に返信する。

## 【0020】

## 【実施例】

(第1実施例) 本発明の第1実施例を図1、図2を用いて説明する。図1において、1は非接触 IC カードの CPU である。

【0021】2はプログラム用の ROM である。3は、CPU の作業用 RAM であり、同時にデータの一時格納エリアでもある。

【0022】4は不揮発性のメモリ (EEPROM) であり、非接触 IC カードが前払い形態の運用をされた場合、電氣的に金額を記憶する財布代わりになるものである。5は Key メモリであり、複数の暗号 Key が格納された領域である。

【0023】6は暗号アルゴリズム実行器である。7は無線インタフェースロジック回路であり、8は無線通信ユニットである。

【0024】本発明の、非接触 IC カードと地上機アンテナで双方に交信されるメッセージは、図2のようになっている。基本構成は、暗号化の際に使用された Key を指し示す Key 番号 (Key インデックス) 9 と、その Key で暗号化された機密データ 10 の集まりで 1 つ

のバケットが構成される事になる。

【0025】まず、地上機は、このバケットを非接触ICカードに送信することになる。これを受信した非接触ICカードでは、まずKey番号の認識を行なう。そして、このKey番号が示すKeyの内容を、暗号アルゴリズム実行器に入力すると同時に、受信した暗号化されたメッセージも一緒に入力する。その出力として平文の認識可能なデータを得ることができるようになる。このような暗号化されたデータから元の平文を再生する動作を復号処理と呼ぶ。

【0026】つまり、地上機のアンテナ制御装置と非接触ICカードの双方で、同じ暗号Keyをもっていなければ、暗号化されたメッセージの解読はできない事になる。これは、この暗号化Keyを知り得ない外部の盗聴者から重要データを保護することに非常に有効な手段となる。

【0027】さらに、非接触ICカードが、地上機アンテナに対して返信する場合も同じであり、まず最初に非接触ICカードは、任意のKey番号を選択し、そのKeyで示されたKeyメモリの内容、すなわち暗号Key自体を、暗号アルゴリズム実行器に入力する。

【0028】それと同時に、送信したいメッセージも一緒に、暗号アルゴリズム実行器に入力する。その結果として、機密Keyで暗号化されたメッセージをえる事ができる。このように、解読可能な平文から機密Keyを用いてメッセージを暗号化する動作を、暗号処理と呼ぶ。

【0029】そして、その任意のKeyと暗号化されたデータをバケットにして、地上機アンテナに返信する事になる。

(第2実施例) 本発明の第2実施例を図3、図4および図5を用いて説明する。

【0030】図3において、101は非接触ICカードのCPUである。102はプログラム用のROMである。103は、CPUの作業用RAMであり、同時にデータの一時格納エリアでもある。

【0031】104は不揮発性のメモリ(EEPROM)であり、非接触ICカードが前払い形態の運用をされた場合、電氣的に金額を記憶する財布代わりになるものである。

【0032】105はKeyメモリであり、複数の暗号Keyが格納された領域である。106は暗号アルゴリズム実行器である。107はランダムナンバー発生器である。

【0033】108は、無線インタフェースロジック回路であり、109は無線通信用ユニットである。これらの一時Key作成過程とデータの暗号化過程を示したものが図4である。図4に示すように、非接触ICカードは最初に、自身でランダムナンバーを発生させる。

【0034】そのランダムナンバーと、任意に選択した

機密Key(マスターKey)を同時に暗号アルゴリズム実行器に入力する。その結果として、一時Keyを得る事ができる。

【0035】次に、その一時Keyと、暗号化したい(被暗号化)データを、同時に暗号アルゴリズム実行器に入力する。その結果として暗号化された機密データを得る事ができるようになる。

【0036】本発明の、非接触ICカードと地上機アンテナの双方に交信されるメッセージは、図5の示すようになっている。基本構成は、暗号化の際に使用されたKeyを指し示すKey番号(Keyインデックス)120と、そのKeyとランダムナンバー121で暗号化関数により作成された一時Keyと、さらにその一時Keyで暗号化された機密データ122の集まりで、1つのバケットが構成される事になる。

【0037】実際のアプリケーションでは、以下のように使用される事になる。まず、地上機は、このバケットを非接触ICカードに送信することになる。これを受信した非接触ICカードでは、まずKey番号の認識を行なう。

【0038】そして、このKey番号が示すKeyの内容を、暗号アルゴリズム実行器に入力すると同時に、受信したランダムナンバーも一緒に入力する。その出力として一時Keyを得ることができる。

【0039】この一時Keyと、受信された機密データを、再度、暗号アルゴリズム実行器に入力することにより、平文の認識可能なデータを得ることができるようになる。このような暗号化されたデータから元の平文を再生する動作を復号処理と呼ぶ。

【0040】つまり、地上機のアンテナ制御装置と非接触ICカードの双方で、同じ暗号Keyをもっていなければ、暗号化されたメッセージの解読はできない事になる。これは、この暗号化Keyを知り得ない外部の盗聴者から重要データを保護することに非常に有効な手段となり得る。

【0041】さらに、非接触ICカードが、地上機アンテナに対して返信する場合も同じであり、まず最初に非接触ICカードは、任意のKey番号を選択し、そのKeyで示されたKeyメモリの内容、すなわち暗号Key自体を、暗号アルゴリズム実行器に入力する。

【0042】それと同時に、非接触ICカードで発生させたランダムナンバーも入力する。その結果として一時Keyを得ることができ、送信したいメッセージとこの一時Keyとを再度、暗号アルゴリズム実行器に入力する。

【0043】その結果として、機密Keyで暗号化されたメッセージを得る事ができる。このように、解読可能な平文から機密Keyを用いてメッセージを暗号化する動作を、暗号処理と呼ぶ。

【0044】そして、その任意のKeyと、ランダムナ

ンバーと暗号化されたデータを、パケットにして、地上機アンテナに返信する事になる。なお、発生させるランダムナンバーの長さは、1バイトよりも複数バイトある方が、作成される一時Keyの展開が豊富であり、データのセキュリティは更に向上する。

#### 【0045】

【発明の効果】本発明は前述のように構成されているので、以下に記載するような効果を奏する。

（請求項1に係る発明の効果）

（1）本発明の非接触ICカードシステムによれば、地上機アンテナと交互に交換されるメッセージ内容は、機密Keyで暗号化されており、盗聴者がそのメッセージをなんらかの形で傍受できたとしても、機密Keyを知り得なければ、有効でかつ意味のあるメッセージに解読できない事になる。

（2）したがって、無線回線上のメッセージのどの部分がどのような意味をなすものなのかを認識する事ができない事になり、その部分をすり替えて、不正に通行料金をごまかそうという行為など、あらゆる不正を防止することができる。

（3）また、本発明の最も効果的な使用方法是、発信されるメッセージ毎に、暗号化のKey、すなわちKey番号を変化させることである。

【0046】これにより、暗号化されたメッセージが幾重にも違った形に展開でき、さらに解読を困難にすることができるようになる。

（請求項2に係る発明の効果）

（1）本発明の非接触ICカードシステムによれば、地上機アンテナと交互に交換されるメッセージ内容は、機密Keyと、ランダムナンバーで、暗号化されており、盗聴者がそのメッセージをなんらかの形で傍受できたとしても、機密Keyを知り得なければ、有効でかつ意味のあるメッセージに解読できない事になる。

（2）したがって、無線回線上のメッセージのどの部分が、どのような意味をなすものなのかを認識する事ができない事になり、その部分をすり替えて、不正に通行料金をごまかそうという行為など、あらゆる不正を防止することができる。

（3）また、本発明の最も効果的な使用方法是、発信されるメッセージ毎に、暗号化のKey、すなわちKey番号を変化させ、更にランダムナンバーで一時的なKeyをえることである。

【0047】これにより、一時Keyも、暗号化されたデータも、無数の広がりをもせ、暗号化されたメッセージが幾重にも違った形に展開でき、さらに解読を困難にすることができるようになる。

【図面の簡単な説明】

【図1】本発明の第1実施例に係る非接触ICカードの構成図。

【図2】本発明の第1実施例に係るパケットの構成図。

【図3】本発明の第2実施例に係る非接触ICカードの構成図。

【図4】本発明の第2実施例に係る暗号化処理ルーチン。

【図5】本発明の第2実施例に係るパケットの構成図。

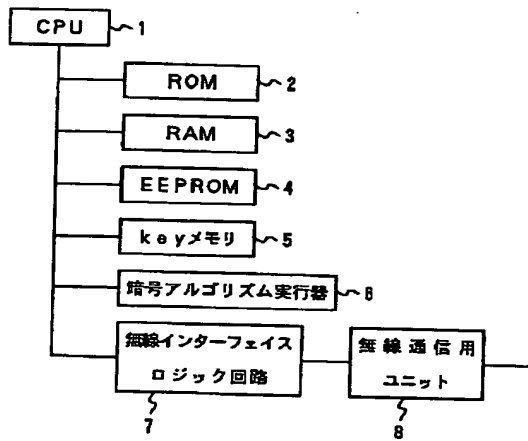
【図6】非接触ICカードの運用イメージ図。

【図7】従来の非接触ICカードの構成図。

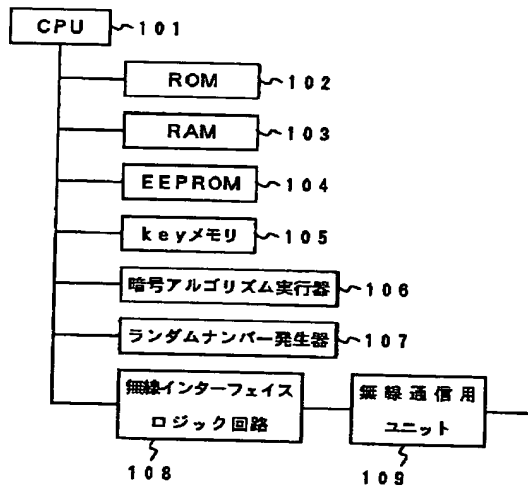
【符号の説明】

- 1…CPU、
- 2…ROM、
- 3…RAM、
- 4…EEPROM、
- 5…Keyメモリ、
- 6…暗号アルゴリズム実行器、
- 7…無線インタフェースロジック回路、
- 8…無線通信ユニット、
- 9…Key番号、
- 10…暗号化されたデータ、
- 11…非接触ICカード、
- 12…車両、
- 13…地上機アンテナが作り出す無線による通信領域、
- 14…地上機アンテナ、
- 15…筐体、
- 16…地上機のアンテナ制御装置、
- 17…料金所ブース、
- 101…CPU、
- 102…ROM、
- 103…RAM、
- 104…EEPROM、
- 105…Keyメモリ、
- 106…暗号アルゴリズム実行器、
- 107…ランダムナンバー発生器、
- 108…無線インタフェースロジック回路、
- 109…無線通信ユニット、
- 113…マスターKey、
- 120…Key番号、
- 121…ランダムナンバー、
- 122…暗号化されたデータ。
- 220…CPU、
- 221…ROM、
- 222…RAM、
- 223…EEPROM、
- 224…無線インタフェースロジック回路、
- 225…無線通信ユニット。

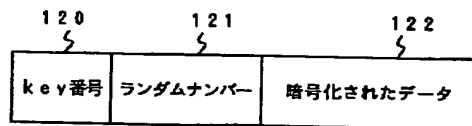
【図1】



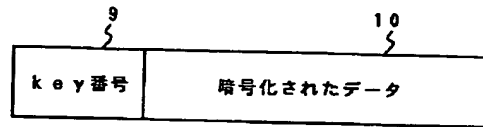
【図3】



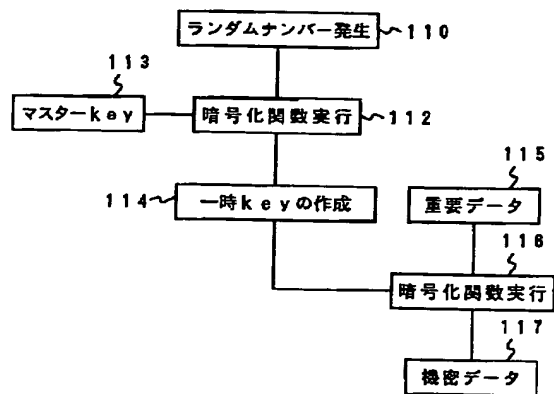
【図5】



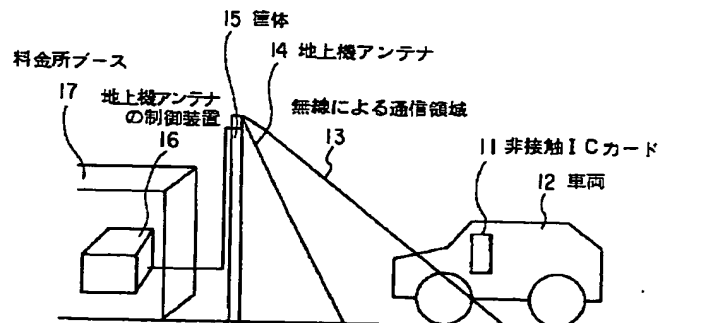
【図2】



【図4】

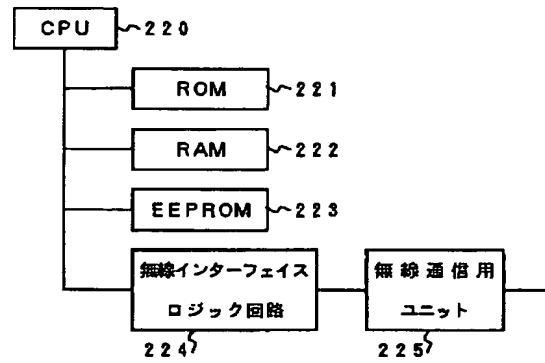


【図6】





【図 7】



フロントページの続き

(51)Int. Cl.<sup>6</sup>

G 0 7 F 7/08  
G 0 8 G 1/017

識別記号

庁内整理番号

F I

G 0 8 G 1/017  
G 0 7 F 7/08

技術表示箇所

S

**THIS PAGE BLANK (USPTO)**